CERTIFICATE OF MAILING

I hereby certify that this correspondence is being mailed, postage paid, to the USPTO at Mail Stop AF, PO Box 1450, Alexandria VA 22313-1450, on March 10, 2006:

John W. Ogilvie

PATENT APPLICATION
Docket No.: 3003.2.10B

UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:	Sanchaita Datta and Ragula Bhaskar
Application No.:	10/034,190
Filed:	December 28, 2001
For:	Domain name resolution making IP address selections in response to connection status when multiple connections are present
Art Unit:	2155
Examiner:	Philip B. Tran

APPELLANTS' BRIEF

(Regarding an Application which has been ***Made Special***)

Honorable Commissioner for Patents:

In response to the final office action mailed February 7, 2006, and pursuant to 37 C.F.R. §§ 41.30 *et seq.*, Applicants respectfully appeal all claim rejections. This application was granted ***accelerated examination*** special status by the Office on June 2, 2003; expedited attention to this brief is called for, and appreciated.

Real Party in Interest

The real party in interest in this appeal is assignee Ragula Systems (FatPipe Networks).

Related Appeals and Interferences

There are no related appeals or interferences.

Status of Claims

Claims 1-10, and 12-21 are pending, are rejected, and are appealed.

Status of Amendments

No claim amendment was filed after final rejection.

Summary of Claimed Subject Matter

The invention provides particular devices, methods, and configured computer-readable storage media for connection-sensitive domain name resolution. Figure 7 directly illustrates methods of the invention, and Figures 1 through 6 directly illustrate systems and devices of the invention. However, the methods help illustrate the devices and configured media, and vice versa; *see, e.g.,* application at page 14 lines 6-9.

Some device embodiments include a data component 114 identifying IP addresses for at least two paths to a server 104 which has a domain name, and a code component 116. The code component receives 702 a domain name resolution request specifying the domain name, selects 704 an IP address based on information about the status of a path to the server but without regard to the server's proximity, and supplies 706 the selected IP address in response to the domain name resolution request, thereby directing traffic to the server over the path. The path status information is obtained at least in part by pinging a router 108 on a path to the server to determine if the router is a reliable connection

component, and may include information such as whether the router answered a ping, when the router was last pinged, and whether no ack was received before timeout for packets sent to the router; *see* application at page 9 line 21 through page 10 line 3. The IP address selection may also be made with status information about connection components other than routers, such as switches, bridges, or packet shapers; *see* application at page 7 lines 14-16.

Grounds of Rejection to be Reviewed on Appeal

The principal two references cited by the rejections are U.S. Patent 6665702 to Zisapel et al. ("Zisapel") and U.S. Patent No. 6779039 to Bommareddy et al. ("Bommareddy"). Also cited are U.S. Patent No. 6262987 to Mogul ("Mogul"), and U.S. Patent No. 6502131 to Vaid et al. ("Vaid").

Rejections were made under 35 U.S.C. § 112 as to the written description, and as to enablement, and also for obviousness under 35 U.S.C. § 103(a).

The grounds of rejection raise these questions for review:

1. Did the Examiner err by making written description rejections without first determining the level of ordinary skill, and without considering descriptive language on page 10 of the application?
2. Did the Examiner err by making enablement rejections without first determining the level of ordinary skill, and without considering language on pages 9-11 of the application?
3. Did the Examiner err by combining Zisapel with Bommareddy without any evidence of a suggestion or motivation in the art to do so?
4. Did the Examiner err by relying on Zisapel and Bommareddy to teach the claimed invention for domain name resolution, when Bommareddy

fails to discuss domain names and Zisapel teaches away from the claimed invention?

Argument

By way of context, the following papers are among those filed by Applicant or mailed by the Office in this case:

Provisional A	provisional application	12/29/2000
Provisional B	provisional application	03/06/2001
Provisional C	provisional application	12/10/2001
Application	non-provisional application	12/28/2001
IDS	information disclosure statement	04/29/2002
Petition	petition for accelerated examination	04/21/2003
Petition Grant	decision granting accelerated examination	06/02/2003
First Action	office action	08/22/2003
First Response	response	02/20/2004
First Final	first "final" office action	05/21/2004
First Appeal	first appeal brief	07/29/2004
Third Party	third party submission re-sent to Examiner	11/23/2004
Reopening Action	office action reopening prosecution	12/03/2004
Second Response	amendment	04/26/2005
Third Action	office action	07/19/2005
Third Response	Amendment	07/25/2005
Second Final	most recent final office action	02/07/2006
Second Appeal	current appeal notice & brief	03/10/2006

The Written Description Rejections are Wrong as a Matter of Law

The Second Final office action asserts on pages 2-3 that the application does not adequately describe making IP address selections without regard to server proximity. The Examiner rejects each independent claim (and thus all claims) under 35 U.S.C. § 112, first paragraph, as lacking the necessary written description.

These written description rejections are clearly erroneous as a matter of law, because the level of ordinary skill was not discussed, much less determined. As explained in M.P.E.P. § 2163.02 "Standard for Determining Compliance With the Written Description Requirement", the adequacy of a description depends on whether it clearly allows "persons of ordinary skill in the art" to recognize that the applicants possessed the claimed invention. The description cannot be analyzed without addressing the level of ordinary skill in the art.

Factors to consider in determining the level of ordinary skill are discussed in M.P.E.P. § 2141.03:

(1) the educational level of the inventor;
(2) type of problems encountered in the art;
(3) prior art solutions to those problems;
(4) rapidity with which innovations are made;
(5) sophistication of the technology; and
(6) educational level of active workers in the field.

The Second Final action fails to even recognize or discuss these factors, much less to present evidence and reasoning in support of some asserted level of ordinary skill. As a matter of law, the written description rejections are therefore clearly erroneous. They should be withdrawn, or reversed on appeal.

If the Examiner chooses to maintain these rejections, or to make any other written description rejection, then he must provide evidence and reasoning that support a determination of the level of ordinary skill. The Examiner has the initial burden of presenting by a preponderance of evidence why a person skilled in the art would not recognize in Applicants' disclosure a description of the invention defined by the claims. In re Wertheim, 541 F.2d 257, 263, 191 USPQ 90, 97 (CCPA 1976). **No evidence** was provided, and very little reasoning. Once the

Examiner has provided enough evidence and reasoning as to the level of ordinary skill to make a *prima facie* case, the undersigned will consider that information, and will then provide rebuttal evidence, arguments, or other responses as appropriate.

The Written Description Rejections are Wrong on the Facts

The Second Final office action fails to acknowledge the following description, which was provided at page 10 lines 14-21 of the application:

> The IP address is selected based on the status of path elements, such as routers 108 and possibly also links 110, where the path element status is defined in terms of path characteristics *such as* the speed of the link, the load on a link, the *hop count* between the requester and the resolver, and/or fixed load distribution. Additional criteria *may* also be considered, such as a pre-defined criterion based on *geographic location* of the requester. The selection should be made, at a minimum, by selecting an IP address for a path that is apparently (based on the data 114) currently available to carry packets. (emphasis added)

Zisapel, which is a principal reference cited by the Examiner, discusses server proximity at many points throughout its specification and claims, including a reference to "measuring proximities" in its Abstract. Zisapel also contains the following in its Background section:

> Where redundant server farms are situated in more than one geographical location, the geographical location of a client may be considered when determining the load balancer to which the client's requests should be routed, in addition to employing conventional load balancing techniques. However, *routing* client requests to the geographically nearest server, load balancer, or server farm might not necessarily provide the client with the best service if, for example, routing the request to a *geographically more distant location* would otherwise result in reduced latency, *fewer hops*, or provide more processing capacity at the server.
> Zisapel, col. 2 lines 8-19 (emphasis added)

Regardless of whatever else may be determined regarding the level of ordinary skill, by citing Zisapel the Examiner presumes that one of ordinary skill is familiar with the concepts discussed in Zisapel. For purposes of this appeal, Applicants agree that hop count and geographic location proximity measures were known to one of ordinary skill.

One of ordinary skill would understand that geographic location and hop count can be used to measure the proximity of a server for routing purposes. One of ordinary skill would also read the excerpt from page 10 of the present application as allowing hop count and/or geographic location to be used as IP address selection criteria, because they are expressly listed there. One of ordinary skill would also understand from page 10 that although proximity criteria can be used, they are not required in every instance, because hop count and geographic location are prefaced by the conditional qualifiers "such as" and "may". Thus, proximity criteria are used in some, but not all, embodiments of the present invention.

In short, one of ordinary skill would understand that IP address selection may be made – in some cases – with regard to proximity to the server. One of skill would also understand, by implication, that in other cases IP address selection is made *without* regard to server proximity. The claims reflect that understanding. Page 10 allows persons of ordinary skill in the art, who would understand hop count and geographic location as proximity measures, to recognize that the Applicants did possess the claimed invention. The written description rejections should be withdrawn, or reversed on appeal.

The Enablement Rejections are Wrong as a Matter of Law

The Second Final office action asserts on pages 4-5 that the application does not enable one of ordinary skill in the art to make and use the invention because undue experimentation would be needed to select an IP address without regard to the proximity of a router or other connection component to the web server. On this basis, the Examiner rejects each independent claim (and thus all claims) under 35 U.S.C. § 112, first paragraph, as non-enabling.

These written description rejections are clearly erroneous as a matter of law, because the level of ordinary skill was not discussed, much less determined. As explained in M.P.E.P. § 2164.01 "Test of Enablement", the adequacy of a description depends on whether it clearly allows "one of ordinary skill in the art" to make and use the claimed invention without undue experimentation. Enablement cannot be analyzed without addressing the level of ordinary skill in the art. As a matter of law, the enablement rejections are therefore clearly erroneous. They should be withdrawn, or reversed on appeal.

Moreover, if the Examiner chooses to maintain these rejections, or to make any other enablement rejection, then he must provide evidence and reasoning that support a determination of the level of ordinary skill. The Examiner has the initial burden when asserting lack of enablement. In re Wright, 999 F.2d 1557, 1562, 27 USPQ2d 1510, 1513 (Fed. Cir. 1993). Once the Examiner has provided enough evidence and reasoning as to the level of ordinary skill to make a *prima facie* case, the undersigned will consider that information, and will then provide rebuttal evidence, arguments, or other responses as appropriate.

The Enablement Rejections are Wrong on the Facts

The Second Final office action fails to acknowledge the discussion of proximity criteria (hop count and geographic location) on page 10 of the application, as discussed above. That language is part of a discussion that also lists several other criteria for selecting IP addresses, including: link speed, link load, load distribution, path availability, link bandwidth, ping results, and other status inquiry results; *see* application at page 10 line 8 through page 11 line 2. Just prior, at application page 9 line 17 through page 10 line 3, other selection criteria are discussed, including router processing speed, router buffer size, whether a router answered a ping, when a router was last pinged, whether a carrier signal is present, and whether packets have been dropped. There may also be other criteria, known in the art, which can be obtained at least in part by pinging.

Most of the IP address selection criteria named in the application are not server proximity criteria. The claimed requirement for selecting an IP address without regard to server proximity can be met by simply minimizing or ignoring the proximity criteria and making the IP address selection depend instead on one or more other criteria. The application provides many other criteria to choose from, including status information obtained at least in part by pinging as claimed.

The Examiner has not met his burden. It is clear that "one reasonably skilled in the art could make or use the invention from the disclosures in the patent coupled with information known in the art without undue experimentation", United States v. Telectronics, Inc., 857 F.2d 778, 785, 8 USPQ2d 1217, 1223 (Fed. Cir. 1988), because DNS resolution can be performed according to the invention using criteria other than proximity criteria. The enablement rejections should be withdrawn, or reversed on appeal.

The Obviousness Rejections Rely on an Improper Combination

The obviousness rejections each rely on a combination of Bommareddy with Zisapel[1]. The Third Response argued that Bommareddy and Zisapel were not properly combined, and that no evidence was given of a suggestion or motivation in the art for combining those references. The next communication from the Examiner, the Second Final action, repeated the rejection and added a single sentence directed to the requirement for evidence. On page 14, in the Examiner's "Response to Arguments" made by Applicants, the Second Final action states:

> It would have been obvious to one of ordinary skill in the art at the time of the invention was made to incorporate the teaching of pinging a router on a path to the server to determine if the router is reliable connection component in the system of router clustering disclosed by Bommareddy into the teaching of load balancing with a connection-sensitive domain name resolution device disclosed by Zisapel in order to efficiently and actively monitor the health of the routers and/or connection paths to the server for detecting a failure and thus re-routing the traffic to the remaining operational router(s) [see Bommareddy, Col. 7, lines 40-62].

The cited portion of Bommareddy reads as follows:

> Another control process is a router monitor that monitors "health" of the routers. In some implementations, the router clustering system 100 monitors router health using a configured polling interval and health check method. The health probe authenticates connectivity of a flow across a router or firewall. In one example the network flow controller 110 periodically sends a Ping packet to router 114, using ICMP extension to confirm that the flow is operative. Router 114 responds on the same port. The Ping packet is sent for each of a plurality of ports.
>
> In some implementations, the router clustering system 100 continually monitors the operational health of the routers and associated wide area network (WAN) links.

1. Vaid and Mogul are added to the Bommareddy-Zisapel combination in rejecting three of the dependent claims.

> In some implementations, the router clustering system 100 detects one or more of various failure conditions. Failures can occur in the router LAN interface and link, or in the router due to power outage, software malfunction, hardware malfunction, or other condition. Failures also can occur in the router WAN interface and link. When the router clustering system 100 detects a failure, traffic is automatically forwarded to the remaining operational router or routers. The router clustering system does not require manual intervention at the server to bypass the failed router. Bommareddy, col. 7, lines 40-62

According to Bommareddy's Abstract and its Summary, a "router clustering system" connects two or more routers to one or more distinct Internet Service Providers (ISPs) in a complete high-availability arrangement. The rejections assert that Bommareddy overcomes an acknowledged deficiency of Zisapel, namely, that Zisapel does not teach pinging a router on a path to a server to determine if the router is a reliable connection component for domain name resolution; *see* Second Final action at page 7. But this is not supported by the cited language of Bommareddy. At most, Bommareddy provides a suggestion or motivation for pinging routers in a router clustering system. The present invention is not directed to router clustering systems. It is directed to domain name resolution. Bommareddy does not discuss domain name resolution.

The Examiner asserts that Bommareddy is "in the same field of load balancing and routing message endeavor" as Zisapel. But "routing message endeavor" is a phrase broad enough to cover every reference that discusses routing, messages, or packet networks – it contains nothing specific to Bommareddy. There is no evidence that one of skill who was familiar with Zisapel would have been motivated to look at Bommareddy. Load balancing, if it is a field rather than a result, is a different one than domain name resolution.

The present application deals with domain name resolution throughout, on each and every page but one (page 19) of its 24 pages of text. Zisapel's text also deals with domain names and DNS in detail and at length, e.g., in at least columns 1, 7 -10, 15, 16. Thus, Zisapel and the present application are each in the field of domain name resolution. Bommareddy, in stark contrast, mentions "DNS" just once, in passing, and Bommareddy fails to discuss "domain name" at all. One who seeks to improve domain name resolution would not have been led to Bommareddy, much less have been motivated to pick out one feature from among the dozens mentioned in Bommareddy.

The Examiner asserts that one of skill would have added Bommareddy to Zisapel "in order to efficiently and actively monitor the health of the routers and/or connection paths to the server for detecting a failure and thus re-routing the traffic to the remaining operational router(s)" Second Final action at 7. But this language is based on the present claims. Zisapel does not mention "health" or "operational" or "failure".

It is perhaps not surprising that Bommareddy would ping routers to check their health when Bommareddy's central thrust is clustering routers. But the present invention is not directed primarily to routers. It is directed to domain name resolution for servers. Conventional solutions have been directed to checking the health of a server when resolving a domain name. The present invention innovates domain name resolution because it checks the *path* to the server. That is not taught by Bommareddy.

The use of Bommareddy was driven by using the claims as a blueprint. Unlike Examiner Tran, who was familiar with Bommareddy because he examined

it, one of ordinary skill in the art of domain name resolution would have had no motivation to consider Bommareddy in combination with Zisapel.

Because there was no suggestion or motivation in the art for combining Zisapel and Bommareddy, the rejections under Section 103 should be withdrawn or reversed.

The Combination Does Not Teach the Claimed Invention

Each of the independent claims requires that IP address selection must now be done without regard to the connection component's proximity to the server. That is, domain name resolution IP address selections which are based primarily or solely on server proximity lie outside the scope of the present claims. *See* claims 1, 8, 13.

Zisapel strongly teaches away from this approach. Zisapel discusses proximity at length, and in depth. Indeed, in the paper copy of Zisapel supplied by the Examiner to the undersigned when Zisapel was first cited, several such portions have hand-written annotations by the Examiner. Among these are portions that discuss proximity and hops (col. 4 lines 58-64), proximity (col. 14 line 41), a proximity table (col. 15 line 25), and best proximity (col. 17 lines 11-17). Language in column 17 lines 6-67 of Zisapel deals with "best proximity connection" and the "number of hops". In short, Zisapel teaches domain name resolution which relies heavily on server proximity as a criterion. By contrast, the present invention performs domain name resolution "without regard" to server proximity.

As noted, Bommareddy teaches nothing specifically about DNS or domain name resolution, much less the very specific claim limitation of assigning IP addresses during domain name resolution without regard to proximity.

Accordingly, even if Bommareddy and Zisapel are considered together, they either fail to teach the present invention, or actually teach away from it. The obviousness rejections should be withdrawn, or reversed on appeal.

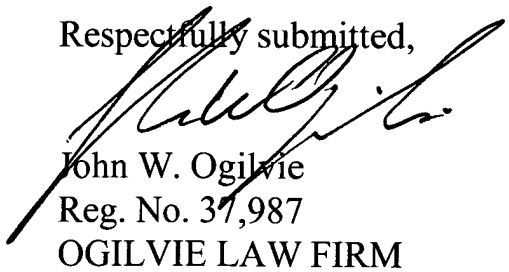
Conclusion

The enablement and written description rejections are erroneous because they have no underlying determination of the level of ordinary skill. They also failed to consider disclosure given in the application. Bommareddy and Zisapel would not have been combined because Bommareddy does not even discuss domain name resolution. In combination, Bommareddy and Zisapel teach away from the invention because Zisapel emphasizes server proximity as a criterion, whereas the invention expressly rules that out. For at least these reasons, the rejections should all be withdrawn or reversed.

Dated March 10, 2006.

\pmAppealBrief-10B

Respectfully submitted,



John W. Ogilvie
Reg. No. 37,987
OGILVIE LAW FIRM
1320 East Laird Avenue
Salt Lake City, UT 84105
801-706-2546 (voice)
801-583-0393 (fax)

Claims Appendix

1. A connection-sensitive domain name resolution device, comprising:

a data component identifying IP addresses for at least two paths to a server which has a domain name; and

a code component which receives a domain name resolution request specifying the domain name, selects an IP address from the data component based on information about the status of a path to the server, said information obtained at least in part by pinging a router on a path to the server to determine if the router is a reliable connection component, said IP address selection made without regard to the router's proximity to the server, and supplies the selected IP address in response to the domain name resolution request.

2. The connection-sensitive domain name resolution device of claim 1, wherein IP addresses in the data component identify routers on paths to the server, and the code component avoids selecting the IP address of a router that is on a path to the server but is not available.

3. The connection-sensitive domain name resolution device of claim 1, wherein IP addresses in the data component identify routers on paths to the server, and the code component selects the IP address in a round-robin manner by selecting the next IP address in a list of IP addresses of routers that are on paths to the server and are available when the selection is made.

4. The connection-sensitive domain name resolution device of claim 1, wherein the code component selects the IP address of an under-loaded path, thereby tending to balance the loads on the paths to the server.

5. The connection-sensitive domain name resolution device of claim 1, wherein the device is placed between the server and a router for the server.

6. The connection-sensitive domain name resolution device of claim 1, in combination with a router for the server, the router having multiple connections to the Internet.

7. The connection-sensitive domain name resolution device of claim 1, in combination with a server-sensitive domain name resolver, wherein the combination performs load-balancing over server paths and also performs load-balancing over multiple servers.

8. A method for distributing domain name resolution results over multiple paths, the method comprising the steps of:

receiving a domain name resolution request which requests an IP address corresponding to a specified domain name;

determining that at least one router is operating reliably and thus is a reliable connection component, by using status information of the router, the status information including at least one of the following: whether the router answered a ping, when the router was last pinged, and whether no ack was received before timeout for packets sent to

the router, the router being in a path to a server having the domain name, the router having an IP address; and

supplying the IP address of the router in a response to the resolution request without regard to the router's proximity to the server, thereby directing traffic to the server over a path through the router.

9. The method of claim 8, further comprising the steps of determining the load on at least one candidate connection component and selecting a connection component which is not over-loaded, the selected connection component having an IP address and being in a path to the server having the domain name, wherein the supplying step comprises sending the IP address of the selected connection component in a response to the resolution request, thereby directing traffic to the server over a path through the connection component that is both reliable and not over-loaded.

10. The method of claim 8, further comprising the step of adjusting the time-to-live to be associated with a DNS record for an IP address in a path to the server.

11. (canceled)

12. The method of claim 8, further comprising the step of performing a router status inquiry to determine the router's load.

13. A computer-readable storage medium having a configuration that will cause performance of a method for connection-sensitive domain name resolution when multiple connections to a web server are potentially available, the method comprising:

receiving a DNS resolution request;

selecting an IP address without regard to a connection component's proximity to the server based on the connection component's status which is determined at least in part by pinging the connection component; and

supplying the selected IP address in response to the request.

14. The configured medium of claim 13, wherein the selecting step comprises determining whether each of at least two routers serving as connection components in a connection responds to pings.

15. The configured medium of claim 13, wherein the selecting step comprises selecting an IP address of the next available path in a round-robin manner.

16. The configured medium of claim 13, wherein the selecting step comprises determining whether a router is under-loaded.

17. The configured medium of claim 13, further comprising the step of setting a DNS record time-to-live.

18. The connection-sensitive domain name resolution device of claim 1, wherein the code component includes code for maintaining logs.

19. The connection-sensitive domain name resolution device of claim 1, wherein the code component includes code for sending alerts to system administrators.

20. The connection-sensitive domain name resolution device of claim 1, wherein the code component includes authentication and security code.

21. The connection-sensitive domain name resolution device of claim 1, wherein the device is configured for multi-homing.

Evidence Appendix
(empty)

Related Proceedings Appendix
(empty)